UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753

22046 7590 09/14/2004

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/578,633	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Office Action

Claims 5 and 25 have been canceled. Claims 1-3, 6-12, 14-24, 26-27 have been fully reconsidered and are pending.

Response to Amendment

Examiner has considered the amendment and has determined that the addition of "the measure of connectivity being an indication of connectivity between the first communications network and the second communications network" renders the claims proper under 35 USC §112. Therefore, that rejection is withdrawn.

Response to Arguments

Applicant has reiterated his stance on the spoofed probe packet by contesting that the he has found a new use for the spoof packet as a probe packet. Examiner is not convinced that this is novel over the teachings of Shostack. Shostack still teaches using a spoof packet to probe the network. Again the Examiner would also point out that spoof is not part of the claimed invention.

Applicant has also alleged that Shostack does not teach utilizing a probe packet to determine a connectivity measure between the two communication network where

the packet includes a source address which is associated with a second communication network. Applicant acknowledges that the probe packet is used to gather a census for a network. Examiner would like to point out the teaching in Shostack in column 13 staring at line 1. Shostack teaches a fourth module of his system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service. Examiner references column 12, lines 41-57 as the teaching of what module two does. Specifically module two carries out the network scan and generates a map of the network and scans the ports for known security vulnerabilities. Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network.

Shostack also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a similar system over a computer network. In line 27, the module invokes remote systems. In line 34, Shostack teaches that this sixth checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions of Shostack's invention.

The examiner has pointed to two separate teachings where Shostack teaches or suggests utilizing a probe packet to determine a connectivity measure between the two communication network where the packet includes a source address which is associated with a second communication network. In view of the foregoing, Examiner maintains the previous 35 USC §102.

Claim Rejections - 35 USC ' 102

Claims 1-3, 6-12, 14-24, and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al (USP 6,298,445).

As per claims 1 and 24, Shostack et al teach a communications network security method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address determined as a function of the topology (column 12, lines 41-57); and

determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claims 2 and 14, Shostack et al teach the source address is an IP address associated with a host external to the communications network (column 1, lines 64-65 and column 3, lines 1-4).

As per claims 3 and 26, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 6, Shostack et al teach the determining the security characteristic operation further comprises:

> monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 7, Shostack et al teach the first and second communications network have different security levels (column 13, lines 1-5).

As per claim 8, Shostack et al teach the transmitted packet is a TCP packet (column 5, lines 24-45).

As per claim 9, Shostack et al teach the second packet is a UDP packet or an ICMP packet (column 5, lines 24-45).

As per claim 10, Shostack et al teach a method for analyzing network security of a communications network, the method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts internal to the communications network as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

transmitting a packet from a host external to the communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet being generated as a function of an IP address associated with the host external to the communications network and an IP address associated with the particular one host of the plurality of hosts internal to the communications network (column 13, lines 1-6); and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet, the security characteristic

being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claim 11, Shostack et al teach the determining the security characteristic operation further comprises:
monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19), the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5).

As per claim 12, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 15, Shostack et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (column 9, lines 10-18).

As per clam 16, Shostack et al teach a communications system comprising:

a first plurality of computers associated with a first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the plurality of computers, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5) performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP address associated with a second computer of the second plurality of computers and an IP address associated with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet (column 12, lines 41-57, column 1, lines 64-65, and column 3, lines 1-4).

As per claim 17, Shostack et al teach the security host computer is associated with the first communications network (column 4, lines 33-34).

As per claim 18, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 19, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claims 20 and 27, Shostack et al teach the first communications network is an intranet and the second communications network is an Internet (column 4, lines 14-21) and the two network communications have different security levels (column 13, lines 1-5).

As per claim 21, Shostack et al teach a security host computer comprising:

means for performing a census of a communications network and determining a topology of a first communications network, the topology being defined by at least one computer (column 12, lines 41-57);

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of the topology, an IP address associated with a particular host computer associated with a second communications network and an IP address associated with the

computer, the second communications network being separate from the first communications network (column 12, lines 41-57); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet (column 12, lines 41-57) the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5).

As per claim 22, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 23, Shostack et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (column 4, lines 14-21).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100